Bösartige Mails erkennen

INFORMATIONS SICHERHEIT

Dringender Ton: "Ihr Account wird gesperrt wenn sie nicht handeln!" – ein typischer Trick, um Druck aufzubauen.

Unbekannter Absender: Der Chef schreibt plötzlich von professormail919@gmail.com statt von einer @tu-freiberg.de Adresse.

Ungewöhnliche Anliegen: "Besorgen sie 50€ Google Play Gutscheine für das Institut als Weihnachtsgeschenk" – gerade wenn es um Geld geht oder um interne Informationen sollten Sie aufmerksam werden!

Zu gut um wahr zu sein: "Sie haben ein Stipendium über 1 Million Euro gewonnen" und ähnlich unseriöse Botschaften sind leider gelogen.

Verdächtige Links: Fahren Sie mit der Maus kurz über den Link, um das wahre Ziel anzuzeigen.

- ✔ https://service.tu-freiberg.de/apps
- ⓘ https://service-tu-freiberg-de.5pdpb.ipfs.dweb.link/apps

Gefährliche Anhänge: "Prüfungsprotokoll.exe" – öffnen Sie keine Anhänge mit ungewöhnlichen Dateiendungen.

Unpersönliche Floskeln: "Sehr geehrter Studierender" statt persönlicher Ansprache mit Ihrem Namen.

Rechtschreibfehler und Grammatik: "Uni Freiburg" oder "Passwort verlohren" sollten Sie bei offiziellen Mails stutzig machen.

Die meisten bösartigen Mails lassen sich enttarnen, wenn man auf sein Bauchgefühl hört: Erscheint eine Nachricht merkwürdig oder untypisch, nehmen Sie sich die Zeit zur Prüfung oder fragen Sie nach!

Wir helfen gerne: **informationssicherheit@tu-freiberg.de**